

On the Sphere Decoding Complexity of STBCs for Asymmetric MIMO Systems

Lakshmi Prasad Natarajan, K. Pavan Srinath and B. Sundar Rajan

Dept. of ECE, IISc, Bangalore 560012, India

Email: {nlp,pavan,bsrajan}@ece.iisc.ernet.in

Abstract—In the landmark paper [1] by Hassibi and Hochwald, it is claimed without proof that the upper triangular matrix \mathbf{R} encountered during the sphere decoding of any linear dispersion code is full-ranked whenever the rate of the code is less than the minimum of the number of transmit and receive antennas. In this paper, we show that this claim is true only when the number of receive antennas is at least as much as the number of transmit antennas. We also show that all known families of high rate (rate greater than 1 complex symbol per channel use) multigroup ML decodable codes have rank-deficient \mathbf{R} matrix even when the criterion on rate is satisfied, and that this rank-deficiency problem arises only in asymmetric MIMO with number of receive antennas less than the number of transmit antennas. Unlike the codes with full-rank \mathbf{R} matrix, the average sphere decoding complexity of the STBCs whose \mathbf{R} matrix is rank-deficient is polynomial in the constellation size. We derive the sphere decoding complexity of most of the known high rate multigroup ML decodable codes and show that for each code, the complexity is a decreasing function of the number of receive antennas.

I. INTRODUCTION

A. System Model and Definitions

We consider Space-Time Block Codes (STBCs) for an N transmit antenna, M receive antenna, quasi-static MIMO channel ($N \times M$ MIMO system) with Rayleigh flat fading. The system can be modeled as

$$\mathbf{Y} = \mathbf{X}\mathbf{H} + \mathbf{W}, \quad (1)$$

where \mathbf{X} is the $T \times N$ codeword matrix transmitted over T channel uses, \mathbf{Y} is the $T \times M$ received matrix, \mathbf{H} is the $N \times M$ channel matrix and the $T \times M$ matrix \mathbf{W} is the additive noise at the receiver. The entries of \mathbf{H} and \mathbf{W} are i.i.d. zero mean, unit variance, circularly symmetric complex Gaussian random variables.

Definition 1: (STBC) An STBC \mathcal{C} encoding K real independent information symbols, denoted by x_i , $i = 1, \dots, K$, is a set of complex matrices given by

$$\mathcal{C} = \left\{ \sum_{i=1}^K x_i \mathbf{A}_i \mid [x_1, \dots, x_K]^T \in \mathcal{A} \right\}, \quad (2)$$

where the $T \times N$ complex matrices $\mathbf{A}_1, \dots, \mathbf{A}_K$, which are called *linear dispersion* or *weight matrices*, are linearly independent over the real field \mathbb{R} [1], [2], and the finite set $\mathcal{A} \subset \mathbb{R}^K$ is called the *signal set*.

Definition 2: (Code Rate) The rate of an STBC is the average number of information symbols transmitted in each

channel use. For the STBC given by (2), the code rate is $R = \frac{K}{T}$ real symbols per channel use, or $R = \frac{K}{2T}$ complex symbols per channel use (cspcu).

The linear independence of the weight matrices in the definition of an STBC implies that $R \leq N$. Throughout this paper, unless otherwise specified, the code rate is taken to be in terms of complex symbols per channel use.

Generally, the signal set \mathcal{A} is chosen in such a way that the STBC \mathcal{C} has full-diversity and large coding gain. In most cases \mathcal{A} is chosen to be a subset of $\Theta \mathbb{Z}^K$, where $\Theta \in \mathbb{R}^{K \times K}$ is a full-ranked matrix. One such instance is when the symbols are partitioned into multiple encoding groups, and each group of symbols is encoded independently of other groups using a lattice constellation, such as in Clifford Unitary Weight Designs [2] (in which case Θ is an orthogonal matrix), Quasi-Orthogonal STBCs [3] and Coordinate Interleaved Orthogonal Designs [4]. There are also instances where the real symbols are encoded independently using regular PAM constellations of possibly different minimum distances [5], in which case Θ is a diagonal matrix with positive entries.

For a complex matrix \mathbf{A} , let its real and imaginary components be denoted by \mathbf{A}_I and \mathbf{A}_Q , respectively. Let $\text{vec}(\mathbf{A})$ denote the complex vector obtained by stacking the columns of \mathbf{A} one below the other and

$$\widetilde{\text{vec}}(\mathbf{A}) \triangleq [\text{vec}(\mathbf{A}_I)^T \text{vec}(\mathbf{A}_Q)^T]^T.$$

Now, the system model given by (1) can be expressed as

$$\mathbf{y} = \widetilde{\text{vec}}(\mathbf{Y}) = \mathbf{G}\mathbf{x} + \mathbf{w},$$

where $\mathbf{x} = [x_1, \dots, x_K]^T$, $\mathbf{w} = \widetilde{\text{vec}}(\mathbf{W})$ and the *equivalent channel matrix* $\mathbf{G} \in \mathbb{R}^{2MT \times K}$ is given by

$$\mathbf{G} = [\widetilde{\text{vec}}(\mathbf{A}_1 \mathbf{H}) \quad \widetilde{\text{vec}}(\mathbf{A}_2 \mathbf{H}) \quad \dots \quad \widetilde{\text{vec}}(\mathbf{A}_K \mathbf{H})].$$

Consider the vector of transformed information symbols $\mathbf{s} = \Theta^{-1} \mathbf{x}$ which takes values from $\mathcal{A}' = \Theta^{-1} \mathcal{A} \subset \mathbb{Z}^K$, where \mathbb{Z} denotes the ring of integers. The components of \mathbf{s} take finite integer values, i.e., $s_i \in \mathcal{A}_q \subset \mathbb{Z}$, with $|\mathcal{A}_q| = q$ for some finite q . Hence one can use a sphere decoder [6] to decode \mathbf{s} and then obtain the ML estimate of the information vector \mathbf{x} . The ML decoder output is given by

$$\hat{\mathbf{s}} = \arg \min_{\mathbf{s} \in \mathcal{A}'} \|\mathbf{y} - \mathbf{G}\Theta \mathbf{s}\|_F^2, \quad (3)$$

where $\|\cdot\|_F$ denotes the Frobenius norm of a matrix.

B. Motivation for our results

It is claimed in [1] without proof that $R \leq \min\{M, N\}$ is a sufficient condition for the system of equations defined by (3) to be *not underdetermined*, i.e., for

$$\text{rank}(\mathbf{G}) = \text{rank}(\mathbf{G}\Theta) = K, \quad \text{with } K \leq 2MT.$$

In Section II, we show that the claim made in [1] is true only for $M \geq N$. This observation is the gateway to the new results presented from Section II onwards.

For a system where $\text{rank}(\mathbf{G}) = K$, the sphere decoder complexity, averaged over noise and channel realizations, is *independent of the constellation size* q and is roughly polynomial in the dimension of the sphere decoding search [6], [7], [8]. However, if the rank of \mathbf{G} is less than K , the average sphere decoding complexity is no more independent of the constellation size. When $\text{rank}(\mathbf{G}) = K' < K$, the conventional sphere decoder needs to be modified as follows [9]: The \mathbf{R} matrix resulting from the **QR**-decomposition of $\mathbf{G}\Theta$ has the form $\mathbf{R} = [\mathbf{R}_a \ \mathbf{R}_b] \in \mathbb{R}^{K' \times K}$, where \mathbf{R}_a is a $K' \times K'$ upper triangular full-rank matrix. There is a corresponding partition of \mathbf{s} as $[\mathbf{s}_a^T \ \mathbf{s}_b^T]^T$. If q is the size of the regular PAM constellation used, then for each of the $q^{K-K'}$ values of \mathbf{s}_b , the conditionally optimal estimate of \mathbf{s}_a can be found by first removing the interference from \mathbf{s}_b , and then using a sphere decoder with the upper triangular matrix \mathbf{R}_a to obtain an estimate of \mathbf{s}_a . Then, from the resulting $q^{K-K'}$ estimates of \mathbf{s} , the optimal vector is chosen. This observation leads to the following lemma.

Lemma 1: For an STBC whose equivalent channel matrix \mathbf{G} is such that $\text{rank}(\mathbf{G}) = K' < K$, the sphere decoding complexity as a function of q is of the order of $q^{K-K'}$, i.e., $\mathcal{O}(q^{K-K'})$.

In the rest of the paper, by sphere decoding complexity we mean the average sphere decoding complexity and the focus is on *the dependence of the complexity on the constellation size* q and *not on the dimension of the sphere decoding search*. We now introduce the notion of *singularity* of an STBC which is a direct indicator of its sphere decoding complexity.

Definition 3: Let \mathcal{C} be an STBC with rate $R = \frac{K}{2T}$ and let $M \geq R$. We say that \mathcal{C} is *singular* for M receive antennas if $\text{rank}(\mathbf{G}) < K$ with probability 1. Otherwise, \mathcal{C} is said to be *non-singular* for M receive antennas.

To illustrate the effect of the rank of \mathbf{G} and singularity of an STBC on the sphere decoding complexity as a function of the constellation size, consider the following example.

Example 1: In [10], a rate $R = \frac{17}{8}$ code for $N = 4$ antennas with $K = 17$ real symbols was presented. Define $\mathbf{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $\mathbf{Z} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, and for any two matrices \mathbf{A}, \mathbf{B} , denote their Kronecker product by $\mathbf{A} \otimes \mathbf{B}$. Then, the 17 weight matrices

$\mathbf{A}_1, \dots, \mathbf{A}_{17}$ of the STBC in [10] are as follows:

$$\begin{aligned} \mathbf{A}_1 &= \mathbf{I}_2 \otimes \mathbf{I}_2, & \mathbf{A}_2 &= i\mathbf{Z} \otimes \mathbf{I}_2, & \mathbf{A}_3 &= \mathbf{Z}\mathbf{X} \otimes \mathbf{I}_2, \\ \mathbf{A}_4 &= i\mathbf{X} \otimes \mathbf{Z}, & \mathbf{A}_5 &= \mathbf{X} \otimes \mathbf{Z}\mathbf{X}, & \mathbf{A}_6 &= i\mathbf{X} \otimes \mathbf{X}, \\ \mathbf{A}_7 &= \mathbf{I}_2 \otimes \mathbf{Z}\mathbf{X}, & \mathbf{A}_8 &= i\mathbf{Z} \otimes \mathbf{X}, & \mathbf{A}_9 &= \mathbf{Z}\mathbf{X} \otimes \mathbf{X}, \\ \mathbf{A}_{10} &= i\mathbf{Z}\mathbf{X} \otimes \mathbf{Z}\mathbf{X}, & \mathbf{A}_{11} &= \mathbf{Z}\mathbf{X} \otimes \mathbf{X}, & \mathbf{A}_{12} &= i\mathbf{X} \otimes \mathbf{I}_2, \\ \mathbf{A}_{13} &= \mathbf{Z} \otimes \mathbf{Z}\mathbf{X}, & \mathbf{A}_{14} &= i\mathbf{I}_2 \otimes \mathbf{X}, & \mathbf{A}_{15} &= i\mathbf{Z} \otimes \mathbf{Z}, \\ \mathbf{A}_{16} &= i\mathbf{I}_2 \otimes \mathbf{I}_2 \quad \text{and} \quad \mathbf{A}_{17} &= i\mathbf{I}_2 \otimes \mathbf{Z}. \end{aligned}$$

Let the number of receive antennas be $M = 3$. Then, $M > R$ and the equivalent channel matrix \mathbf{G} is of size 24×17 . Now consider the following randomly generated channel matrix

$$\mathbf{H} = \begin{bmatrix} 0.3457 + 0.2299i & 0.2078 - 0.0723i & -0.7558 - 0.6116i \\ 0.7316 - 0.5338i & -0.5567 - 0.1707i & -0.5724 - 0.0212i \\ 0.5140 + 0.9689i & 0.6282 + 0.2257i & -2.0819 - 0.1166i \\ -0.2146 - 1.2102i & -0.8111 + 0.2212i & 1.0171 + 0.4439i \end{bmatrix}.$$

The resulting \mathbf{G} matrix has rank only 16 and the structure of the upper triangular matrix \mathbf{R} of size 24×17 obtained upon its **QR**-decomposition is shown in (4) at the top of next page. The non-zero entries of \mathbf{R} are denoted by ' a '. It is clear that the first 16 columns of \mathbf{R} are linearly independent and the last column lies in the span of the first 16 columns. Removing the last 8 rows of \mathbf{R} , which are all zeros, we get the 16×17 real matrix \mathbf{R}' which is used by the sphere decoder to find the ML estimate of the information vector. In this case, from Lemma 1, the complexity of sphere decoding this STBC for this particular channel realization \mathbf{H} is of the order of $q^{17-16} = q$. In Section III-A, by establishing that $\text{rank}(\mathbf{G}) = 16$ with probability 1, we show that this STBC is singular for $M = 3$.

C. Contributions of the Paper

The contributions and organization of this paper are as follows.

- We introduce the notion of singularity of an STBC which is a direct indicator of its sphere decoding complexity.
- We show that contrary to the claim made in [1], $R \leq \min\{M, N\}$ is not a sufficient condition for an STBC to be non-singular for M receive antennas (Theorem 1, Section II). We show that the case of singular STBCs arises only for asymmetric MIMO systems with $M < N$ (Proposition 1, Section II).
- We show that all known families of high rate ($R > 1$) multigroup ML decodable¹ codes [10], [11], [12], [13] and [14] are non-singular for certain values of M (Section III, see Table I for a summary of results).
- We derive the sphere decoding complexity of almost all known high-rate multigroup ML decodable codes and show that in each case the sphere decoding complexity is a decreasing function of the number of receive antennas M (Section III, see Table I). We show that even when an STBC is singular, multigroup ML decodability helps reduce the sphere decoding complexity. The reduction in

¹An STBC is g -group or multigroup ML decodable if its symbols can be partitioned into g groups and each group of symbols can be ML decoded independent of others.

$$\mathbf{R} = \begin{bmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a & 0 & 0 & 0 & 0 & a & a & 0 & 0 & 0 & 0 & a & a & a & a & a \\ 0 & 0 & a & 0 & 0 & 0 & a & 0 & a & a & a & 0 & 0 & a & 0 & a & a \\ 0 & 0 & 0 & a & 0 & 0 & 0 & a & a & a & 0 & a & a & 0 & 0 & a & a \\ 0 & 0 & 0 & 0 & a & 0 & a & a & a & 0 & a & a & 0 & 0 & a & a & 0 \\ 0 & 0 & 0 & 0 & 0 & a & 0 & 0 & 0 & a & a & a & a & a & a & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & a & a & a & a & a & a & a & a & a & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a & a & a & a & a & a & a & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a & a & a & a & a & a & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a & a & a & a & a & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a & a & a & a & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a & a & a & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a & a & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (4)$$

complexity is from $\mathcal{O}(q^{K-K'})$ to $\mathcal{O}(q^{\frac{K-K'}{g}})$, where g is the number of ML decoding groups (Section III).

Some related open problems are discussed in Section IV.

Notations: Throughout the paper, matrices (vectors) are denoted in bold, uppercase (lowercase) letters. For a complex matrix \mathbf{A} , its transpose, conjugate and conjugate-transpose are denoted by \mathbf{A}^T , $\bar{\mathbf{A}}$ and \mathbf{A}^H , respectively. For a square matrix \mathbf{A} , $\det(\mathbf{A})$ denotes its determinant. The $n \times n$ identity matrix is denoted by \mathbf{I}_n and $\mathbf{0}$ is the null matrix of appropriate dimension. Unless used as a subscript or to denote indices, $i = \sqrt{-1}$. For square matrices \mathbf{A}_j , $j = 1, \dots, d$, $\text{diag}(\mathbf{A}_1, \dots, \mathbf{A}_d)$ denotes the square, block-diagonal matrix with $\mathbf{A}_1, \dots, \mathbf{A}_d$ on the diagonal, in that order. The field of complex numbers is denoted by \mathbb{C} .

II. BASIC RESULTS ON THE RANK OF THE EQUIVALENT CHANNEL MATRIX

We present a few results which we will use in the following sections to derive the rank of \mathbf{G} for specific STBCs. The following result shows that if any STBC is singular for M receive antennas, then $M < N$. Thus, the rank-deficiency problem arises only in asymmetric MIMO with $M < N$.

Proposition 1: If $M \geq N$, every $T \times N$ STBC is non-singular for M receive antennas.

Proof: Since $\widetilde{\text{vec}}(\cdot)$ is an isomorphism from the \mathbb{R} -vector space $\mathbb{C}^{T \times M}$ to \mathbb{R}^{2MT} , it is enough to show that $\mathbf{A}_1\mathbf{H}, \dots, \mathbf{A}_K\mathbf{H}$ are linearly independent with probability 1. Suppose \mathbf{H} is full-ranked, i.e., $\text{rank}(\mathbf{H}) = N$, then there exists a matrix $\mathbf{H}^\dagger \in \mathbb{C}^{M \times N}$ such that $\mathbf{H}\mathbf{H}^\dagger = \mathbf{I}_N$. If $\mathbf{V} =$

$\sum_{i=1}^K a_i \mathbf{A}_i \mathbf{H} = \mathbf{0}$, it would mean that $\mathbf{V}\mathbf{H}^\dagger = \sum_{i=1}^K a_i \mathbf{A}_i = \mathbf{0}$. Since \mathbf{A}_i are the weight matrices of an STBC, they are linearly independent and hence $a_i = 0$, $i = 1, \dots, K$. Thus $\text{rank}(\mathbf{G}) = K$ if \mathbf{H} is full-ranked. Since \mathbf{H} is full-ranked with probability 1 [15], we have shown that any STBC is non-singular for M receive antennas if $M \geq N$. ■

Let $\langle \mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_K \rangle$ denote the \mathbb{R} -linear subspace of $\mathbb{C}^{T \times N}$ spanned by the matrices $\mathbf{A}_1, \dots, \mathbf{A}_K$.

Proposition 2: Let $\mathbf{B}_1, \dots, \mathbf{B}_K$ be $T \times N$ complex matrices such that $\langle \mathbf{A}_1, \dots, \mathbf{A}_K \rangle = \langle \mathbf{B}_1, \dots, \mathbf{B}_K \rangle$ and let $\mathbf{H} \in \mathbb{C}^{N \times M}$ be any matrix. Then the column spaces of the matrices

$$\mathbf{G}_\mathbf{A}(\mathbf{H}) = [\widetilde{\text{vec}}(\mathbf{A}_1\mathbf{H}) \ \widetilde{\text{vec}}(\mathbf{A}_2\mathbf{H}) \ \dots \ \widetilde{\text{vec}}(\mathbf{A}_K\mathbf{H})] \text{ and} \quad (5)$$

$$\mathbf{G}_\mathbf{B}(\mathbf{H}) = [\widetilde{\text{vec}}(\mathbf{B}_1\mathbf{H}) \ \widetilde{\text{vec}}(\mathbf{B}_2\mathbf{H}) \ \dots \ \widetilde{\text{vec}}(\mathbf{B}_K\mathbf{H})] \quad (6)$$

are identical. In particular, $\text{rank}(\mathbf{G}_\mathbf{A}(\mathbf{H})) = \text{rank}(\mathbf{G}_\mathbf{B}(\mathbf{H}))$.

Proof: Let \mathbf{v} be any vector in the column space of $\mathbf{G}_\mathbf{A}(\mathbf{H})$. Then, $\mathbf{v} = \sum_{i=1}^K a_i \widetilde{\text{vec}}(\mathbf{A}_i\mathbf{H})$, for some choice of real numbers a_i , $i = 1, \dots, K$. Since each of the $\mathbf{A}_i \in \langle \mathbf{B}_1, \dots, \mathbf{B}_K \rangle$, every \mathbf{A}_i can be written as some real linear combination of $\mathbf{B}_1, \dots, \mathbf{B}_K$. It follows that every $\widetilde{\text{vec}}(\mathbf{A}_i\mathbf{H})$ can be written as some real linear combination of $\widetilde{\text{vec}}(\mathbf{B}_1\mathbf{H}), \dots, \widetilde{\text{vec}}(\mathbf{B}_K\mathbf{H})$. Hence \mathbf{v} belongs to the column space of $\mathbf{G}_\mathbf{B}(\mathbf{H})$. Similarly we can show that every vector in the column space of $\mathbf{G}_\mathbf{B}(\mathbf{H})$ belongs to the column space of $\mathbf{G}_\mathbf{A}(\mathbf{H})$ also. This completes the proof. ■

The following result shows that if every weight matrix of a given STBC is multiplied on the left by a constant invertible matrix, then the rank of the equivalent channel matrix is unchanged.

Proposition 3: Let $\mathbf{C} \in \mathbb{C}^{T \times T}$ be any full-rank matrix, $\mathbf{B}_i = \mathbf{C}\mathbf{A}_i$, $i = 1, \dots, K$ and \mathbf{H} be any $N \times M$ complex matrix. Then we have $\text{rank}(\mathbf{G}_\mathbf{A}(\mathbf{H})) = \text{rank}(\mathbf{G}_\mathbf{B}(\mathbf{H}))$, where $\mathbf{G}_\mathbf{A}(\mathbf{H})$ and $\mathbf{G}_\mathbf{B}(\mathbf{H})$ are as defined in (5) and (6).

Proof: It suffices to show that the subspaces $\langle \mathbf{A}_1\mathbf{H}, \dots, \mathbf{A}_K\mathbf{H} \rangle$ and $\langle \mathbf{C}\mathbf{A}_1\mathbf{H}, \dots, \mathbf{C}\mathbf{A}_K\mathbf{H} \rangle$ have the same dimension. The proof is complete if we show that the vector space homomorphism φ from the former subspace to the latter, that sends $\mathbf{V} = \sum_{i=1}^K a_i \mathbf{A}_i \mathbf{H}$ to $\sum_{i=1}^K a_i \mathbf{C}\mathbf{A}_i \mathbf{H}$ is a one to one map. If $\mathbf{V} \in \ker(\varphi)$, then $\varphi(\mathbf{V}) = \mathbf{C} \sum_{i=1}^K a_i \mathbf{A}_i \mathbf{H} = \mathbf{C}\mathbf{V} = \mathbf{0}$. Since \mathbf{C} is invertible, this means that $\mathbf{V} = \mathbf{0}$. This completes the proof. ■

It is shown in [14] that for any $N \geq 1$, there exists an explicitly constructable set of N^2 matrices belonging to $\mathbb{C}^{N \times N}$ that are unitary, Hermitian and linearly independent over \mathbb{R} . This set of matrices forms a basis for the space of $N \times N$ Hermitian matrices. Denote by $\mathcal{C}_N^{\text{Herm}}$ any STBC obtained by using these N^2 matrices as weight matrices. For positive integers n and m , define the function

$$f(n, m) = n^2 - ((n - m)^+)^2,$$

where $(a)^+ = \max\{a, 0\}$. We now state the main result of this paper.

Theorem 1: The equivalent channel matrix of the STBC $\mathcal{C}_N^{\text{Herm}}$ for M receive antennas has rank $f(N, M)$ with probability 1.

Proof: See Appendix A. ■

The rate of $\mathcal{C}_N^{\text{Herm}}$ is $\frac{N}{2}$ and the rank of the equivalent channel is less than $K = N^2$ whenever $M < N$. Thus, this STBC is singular for all $\frac{N}{2} \leq M < N$.

Example 2: Consider the STBC $\mathcal{C}_3^{\text{Herm}}$ used in an asymmetric MIMO system with $M = 2$ receive antennas. In this case, $R = \frac{3}{2} < \min\{M, N\}$ and the equivalent channel matrix \mathbf{G} is of size 12×9 . From Theorem 1, we know that the rank of \mathbf{G} is equal to $f(3, 2) = 8$ with probability 1. Hence, this STBC is singular for 2 receive antennas. The 9 weight matrices of the STBC $\mathcal{C}_3^{\text{Herm}}$ are as follows

$$\mathbf{A}_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \mathbf{A}_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \mathbf{A}_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix},$$

$$\mathbf{A}_4 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \mathbf{A}_5 = \begin{bmatrix} 0 & i & 0 \\ -i & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \mathbf{A}_6 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix},$$

$$\mathbf{A}_7 = \begin{bmatrix} 0 & 0 & i \\ 0 & 1 & 0 \\ -i & 0 & 0 \end{bmatrix}, \mathbf{A}_8 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \text{ \& } \mathbf{A}_9 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & i \\ 0 & -i & 0 \end{bmatrix}.$$

The structure of the 12×9 upper triangular matrix R' obtained from the QR decomposition of \mathbf{G} when \mathbf{H} equals the following randomly generated matrix

$$\begin{bmatrix} -0.5688 - 0.8117i & -0.1723 + 1.8282i \\ 0.4926 + 0.0742i & 0.1525 - 0.4716i \\ 0.5905 + 0.5107i & -0.8244 + 0.1325i \end{bmatrix},$$

is given by

$$R' = \begin{bmatrix} a & a & a & a & a & a & a & a & a \\ 0 & a & a & a & a & a & a & a & a \\ 0 & 0 & a & a & a & a & a & a & a \\ 0 & 0 & 0 & a & a & a & a & a & a \\ 0 & 0 & 0 & 0 & a & a & a & a & a \\ 0 & 0 & 0 & 0 & 0 & a & a & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & a & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

The sphere decoder uses the 8×9 matrix R obtained from R' by deleting its last 4 rows which are all zero. Hence, for this particular channel realization \mathbf{H} , the sphere decoding complexity is of the order of $q^{9-8} = q$.

The remaining part of this section is concerned with multi-group ML decodable codes. Suppose the code obtained from an STBC \mathcal{C} with a signal set \mathcal{A} is g -group ML decodable for some $g > 1$. The information symbols $\{x_1, \dots, x_K\}$ can be partitioned into g vectors $\mathbf{x}_{\mathcal{I}_1}, \dots, \mathbf{x}_{\mathcal{I}_g}$ of length $\lambda_1, \dots, \lambda_g$ respectively such that each symbol vector can be ML decoded independently of other symbol vectors. There is a corresponding partition of the channel matrix into g submatrices $\mathbf{G}_1, \dots, \mathbf{G}_g$, such that

$$\mathbf{G}\mathbf{x} = \sum_{k=1}^g \mathbf{G}_k \mathbf{x}_{\mathcal{I}_k}, \quad \mathbf{G}_k \in \mathbb{R}^{2MT \times \lambda_k}, \quad \text{for } k = 1, \dots, g. \quad (7)$$

In Theorem 2 of [16] it is shown that for any $k \neq k'$ and any channel realization \mathbf{H} , every column of \mathbf{G}_k is orthogonal to every column of $\mathbf{G}_{k'}$. As a direct consequence of this, we have the following proposition.

Proposition 4: For any g -group ML decodable STBC and any channel realization \mathbf{H} , $\text{rank}(\mathbf{G}) = \sum_{k=1}^g \text{rank}(\mathbf{G}_k)$.

Proof: Since the column spaces of \mathbf{G}_k , $k = 1, \dots, g$ are orthogonal to each other, the dimension of the column space of \mathbf{G} is equal to the sum of the dimensions of the column spaces of \mathbf{G}_k , $k = 1, \dots, g$. ■

III. SPHERE DECODING COMPLEXITY OF SOME KNOWN FAMILIES OF CODES

In this section, we show that all known families of high-rate ($R > 1$) multigroup ML decodable codes are singular for certain number of receive antennas. Using the properties of the rank of the equivalent channel matrix derived in the previous section, we now derive the sphere decoding complexities of these known multigroup ML decodable STBCs. Table I summarizes the results of this section. The table lists the sphere decoding complexity and the minimum number of receive antennas for non-singularity of $\mathcal{C}_N^{\text{Herm}}$, the codes in [10], [12], [13], and the codes in [14] corresponding to even number of ML decoding groups.

TABLE I
COMPARISON OF SPHERE DECODING COMPLEXITIES OF KNOWN SINGULAR STBCs

Code	Transmit Antennas N	Delay T	Groups g	Rate (cspcu) R	Minimum M for non-singularity	Order of Sphere Decoding Complexity Exponent of $q^{\dagger,*}$
\mathcal{C}_N^{Herm} (Theorem 1)	≥ 1	N	1	$\frac{N}{2}$	N	$((N - M)^+)^2$
Ren et. al. [10]	4	4	2	$\frac{17}{8}$	4	$((4 - M)^+)^2$
Ren et al. [12]	≥ 1	$\geq 2N$	2	$N - \frac{N^2-1}{T}$	N	$(N - M)^+ \cdot (T - N - M)$
Srinath et al. [13]	$2^m, m \geq 2$	N	2	$\frac{N}{4} + \frac{1}{N}$	$\frac{N}{2}$	$((\frac{N}{2} - M)^+)^2$
Natarajan et. al. [14] [‡]	$ng2^{\lfloor \frac{g-1}{2} \rfloor}, n \geq 1$	N	$2\ell, \ell \geq 1$	$\frac{N}{g2^{g-1}} + \frac{g^2-g}{2N}$	$\frac{N}{g2^{g-2}}$	$\left(\left(\frac{N}{g2^{\lfloor \frac{g-1}{2} \rfloor}} - 2^{\lfloor \frac{g-1}{2} \rfloor} M \right)^+ \right)^2$
	$n2^{\lfloor \frac{g-1}{2} \rfloor}, n \geq 1$	gN	$2\ell, \ell \geq 1$	$\frac{N}{2^{g-1}} + \frac{g-1}{2N}$	$\frac{N}{2^{g-2}}$	$\left(\left(\frac{N}{2^{\lfloor \frac{g-1}{2} \rfloor}} - 2^{\lfloor \frac{g-1}{2} \rfloor} M \right)^+ \right)^2$

[†] The size of the real constellation used is denoted by q .

^{*} For any real number a , a^+ is defined as $\max\{a, 0\}$.

[‡] [14] contains codes for all $g > 1$ and not just even values of g .

A. Fast-group-decodable STBC from Ren et. al. [10]

In [10], a 2-group decodable STBC for 4 transmit antennas with $R = 17/8$ was constructed. For this code, with the notations as used in (7), $\mathbf{x}_{\mathcal{I}_1} = x_1$, $\lambda_1 = 1$, $\mathbf{x}_{\mathcal{I}_2} = [x_2, \dots, x_{16}]^T$, $\lambda_2 = 16$ and $\mathbf{G} = [\mathbf{G}_1 \ \mathbf{G}_2]$. The weight matrix corresponding to x_1 is \mathbf{I}_4 . Since any two weight matrices from different groups are Hurwitz-Radon orthogonal, i.e., satisfy $\mathbf{A}_i^H \mathbf{A}_j + \mathbf{A}_j^H \mathbf{A}_i = \mathbf{0}$, all the matrices in the second group must be skew-Hermitian, i.e., $\mathbf{A}_i^H = -\mathbf{A}_i$, $i = 2, \dots, 17$. As a result, we can express these weight matrices as $\mathbf{A}_i = i\mathbf{I}_4 \mathbf{A}_i'$, $i = 2, \dots, 17$, with \mathbf{A}_i' being Hermitian matrices. It is clear that for any arbitrary channel realization \mathbf{H} , $\mathbf{G}_1 = [\vec{vec}(\mathbf{H})]$ which is non-zero with probability 1. Hence, $\text{rank}(\mathbf{G}_1) = 1$ with probability 1. From Proposition 3 and Theorem 1, $\text{rank}(\mathbf{G}_2) = f(4, M)$ with probability 1. So,

- 1) for $M = 3$, $\text{rank}(\mathbf{G}_2) = 15$. Since $\mathbf{x}_{\mathcal{I}_1}$ and $\mathbf{x}_{\mathcal{I}_2}$ can be decoded independently of each other, from Proposition 3, the sphere decoding complexity of the first group is independent of q while that of the second group is $\mathcal{O}(q^{(16-15)}) = \mathcal{O}(q)$. Consequently, the sphere decoding complexity of the code in [10] is $\mathcal{O}(q)$ for 3 receive antennas.
- 2) For $M \geq 4$, $f(4, M) = 16$ and the STBC in [10] is non-singular for 4 or more receive antennas. Hence, its sphere decoding complexity is independent of q .

B. High-rate 2-group ML decodable codes from Srinath et. al. [13]

A family of 2-group ML decodable STBCs was constructed in [13] for $N = 2^m$, $m > 1$ antennas with rate $R = \frac{N}{4} + \frac{1}{N}$ cspcu. This family includes the rate $\frac{5}{4}$ code of [11] for $N = 4$ as a special case. The number of symbols in the STBC is $K = \frac{N^2}{2} + 2$. In the rest of this subsection we show that the sphere decoding complexity is $\mathcal{O}\left(q^{\left((\frac{N}{2}-M)^+\right)^2}\right)$ which is polynomial in q , and so is large for all $\lceil R \rceil \leq M < \frac{N}{2}$, where

$\lceil a \rceil$ is the smallest integer greater than or equal to a . Note that the sphere decoding complexity is a decreasing function of the number of receive antennas M .

Derivation of sphere decoding complexity: The STBCs constructed in [13] have a block diagonal structure. The weight matrices for $N = 2^m$ antennas are of the form $\text{diag}(\mathbf{V}_1, \mathbf{V}_2)$, where $\mathbf{V}_1, \mathbf{V}_2 \in \mathbb{C}^{n \times n}$ are unitary and $n = \frac{N}{2}$. Noting that the STBC is 2-group decodable, denote the set of weight matrices belonging to the first and the second group by \mathcal{G}_1 and \mathcal{G}_2 , respectively. For all the matrices in \mathcal{G}_1 , \mathbf{V}_1 is constant, say \mathbf{F}_1 , and for all the matrices in \mathcal{G}_2 , \mathbf{V}_2 is constant, say \mathbf{F}_2 . Each group contains $n^2 + 1$ real symbols. We will now derive the rank of the submatrix \mathbf{G}_1 of \mathbf{G} that corresponds to \mathcal{G}_1 .

Let $\mathcal{G}_1 = \{\mathbf{A}_1, \dots, \mathbf{A}_{n^2+1}\}$. Consider the set

$$\mathcal{G}'_1 = \{\mathbf{A}'_i = \mathbf{C}\mathbf{A}_i, i = 1, \dots, n^2 + 1\},$$

where $\mathbf{C} = \text{diag}(\mathbf{I}_n, i\mathbf{F}_2^H)$. Since \mathbf{C} is unitary, from Proposition 3, the rank of \mathbf{G}_1 equals the rank of \mathbf{G}'_1 , the equivalent channel matrix corresponding to \mathcal{G}'_1 . Since the multiplication of all the weight matrices of an STBC by a unitary matrix does not affect its multigroup ML decodability, for any matrix \mathbf{B} belonging to \mathcal{G}_2 and any $j = 1, \dots, n^2 + 1$, we have

$$\mathbf{A}'_j{}^H (\mathbf{C}\mathbf{B}) + (\mathbf{C}\mathbf{B})^H \mathbf{A}'_j = \mathbf{0}, \quad (8)$$

where \mathbf{A}'_j and $\mathbf{C}\mathbf{B}$ are block diagonal and are of the form

$$\mathbf{A}'_j = \begin{bmatrix} \mathbf{F}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{D}_j \end{bmatrix} \text{ and } \mathbf{C}\mathbf{B} = \begin{bmatrix} \mathbf{V} & \mathbf{0} \\ \mathbf{0} & i\mathbf{I}_n \end{bmatrix},$$

for some unitary matrices \mathbf{D}_j and \mathbf{V} . Since \mathbf{A}'_j and $\mathbf{C}\mathbf{B}$ satisfy (8) and are block diagonal, from Lemma 1 of [13], $\mathbf{D}_j^H i\mathbf{I}_n + (i\mathbf{I}_n)^H \mathbf{D}_j = \mathbf{0}$. Thus, for $j = 1, \dots, n^2 + 1$, \mathbf{D}_j is a $n \times n$ unitary, Hermitian matrix. Next we use Proposition 2 to find the rank of \mathbf{G}'_1 .

Note that $\langle \mathbf{A}'_1, \dots, \mathbf{A}'_{n^2+1} \rangle$ is same as the span of

$$\begin{bmatrix} \mathbf{F}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}, \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{D}_1 \end{bmatrix}, \dots, \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{D}_{n^2+1} \end{bmatrix}. \quad (9)$$

Since $\mathbf{A}_1, \dots, \mathbf{A}_{n^2+1}$ are linearly independent, $\mathbf{A}'_1, \dots, \mathbf{A}'_{n^2+1}$ are also linearly independent. Further, the first matrix in (9) is linearly independent of the remaining matrices and hence the dimension of the span of the remaining matrices in (9) is n^2 . Without loss of generality, let us assume that $\mathbf{D}_1, \dots, \mathbf{D}_{n^2}$ are linearly independent, thus $\langle \mathbf{D}_1, \dots, \mathbf{D}_{n^2} \rangle$ is the space of all $n \times n$ Hermitian matrices. Then, $\langle \mathbf{A}'_1, \dots, \mathbf{A}'_{n^2+1} \rangle$ equals the space spanned by

$$\begin{bmatrix} \mathbf{F}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}, \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{D}_1 \end{bmatrix}, \dots, \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{D}_{n^2} \end{bmatrix}. \quad (10)$$

From Proposition 2, it is enough if we concentrate on the STBC whose weight matrices are given by (10). Let the channel matrix be partitioned as $\mathbf{H} = \begin{bmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \end{bmatrix}$, where $\mathbf{H}_1, \mathbf{H}_2 \in \mathbb{C}^{n \times M}$. We need to compute the dimension of the space spanned by the weight matrices multiplied on the right by \mathbf{H} which is

$$\left\langle \begin{bmatrix} \mathbf{F}_1 \mathbf{H}_1 \\ \mathbf{0} \end{bmatrix}, \begin{bmatrix} \mathbf{0} \\ \mathbf{D}_1 \mathbf{H}_2 \end{bmatrix}, \dots, \begin{bmatrix} \mathbf{0} \\ \mathbf{D}_{n^2} \mathbf{H}_2 \end{bmatrix} \right\rangle.$$

With probability 1, \mathbf{H}_1 is non-zero and hence the first matrix is linearly independent of the remaining matrices. From Theorem 1, the dimension of the span of the remaining n^2 matrices is $f(n, M) = n^2 - ((n - M)^+)^2$ with probability 1. Thus $\text{rank}(\mathbf{G}_1)$ equals $f(n, M) + 1$ with probability 1. A similar result can also be proved for the second ML decoding group, i.e., for $\text{rank}(\mathbf{G}_2)$. From Proposition 4, $\text{rank}(\mathbf{G}) = \text{rank}(\mathbf{G}_1) + \text{rank}(\mathbf{G}_2)$ which equals

$$K' = 2 \left(\frac{N^2}{4} - \left(\left(\frac{N}{2} - M \right)^+ \right)^2 + 1 \right).$$

Comparing this with $K = 2 \left(\frac{N^2}{4} + 1 \right)$, we see that the STBC given in [13] is non-singular only if $M \geq \frac{N}{2} \approx 2R$. Hence the code is singular for all $\lceil R \rceil \leq M < \frac{N}{2}$.

Now, the two groups of symbols can be ML decoded independently of each other, and the number of symbols in each group is $\frac{K}{2}$, with $\text{rank}(\mathbf{G}_1) = \text{rank}(\mathbf{G}_2) = \frac{K'}{2}$. Thus, the sphere decoding complexity of the STBC is $\mathcal{O} \left(q^{\frac{K-K'}{2}} \right)$ instead of $\mathcal{O} \left(q^{K-K'} \right)$. Hence, *multigroup ML decodability reduces the sphere decoding complexity even if the STBC is singular.*

C. Two group ML decodable codes from Ren et. al. [12]

In [12], 2-group ML decodable codes for all $N \geq 1$ and all even $T \geq 2N$ were constructed with rate $R = N - \frac{N^2-1}{T}$. The number of symbols per group is $\frac{K}{2} = TN - N^2 + 1$. In this subsection, we show that the codes of this family are singular for all $\lceil R \rceil \leq M < N$ receive antennas and that their sphere decoding complexity is $\mathcal{O} \left(q^{(N-M)^+ \cdot (T-N-M)} \right)$. Using Proposition 1, it is clear that these codes are non-singular if and only if $M \geq N$.

Derivation of sphere decoding complexity: The structure and derivation of the sphere decoding complexity of these codes is similar to that of the codes from [13], which was discussed in Section III-B. The weight matrices of the STBCs in [12] are of the form $\begin{bmatrix} \mathbf{V}_1 \\ \mathbf{V}_2 \end{bmatrix}$, where $\mathbf{V}_1, \mathbf{V}_2 \in \mathbb{C}^{\frac{T}{2} \times N}$. For all the matrices in the first group, $\mathbf{V}_1 = \pm \mathbf{F}_1$ for some constant matrix \mathbf{F}_1 , and for all the matrices in the second group, $\mathbf{V}_2 = \pm \mathbf{F}_2$ for some constant matrix \mathbf{F}_2 . The STBCs constructed in [12] are such that for each $k = 1, 2$, the \mathbf{V}_k submatrices of any two weight matrices belonging to different groups are Hurwitz-Radon orthogonal. We consider the case where \mathbf{F}_k , $k = 1, 2$ are semi-unitary i.e., $\mathbf{F}_k^H \mathbf{F}_k = \mathbf{I}_N$. We derive the sphere decoding complexity only for the first group. Using a similar argument the complexity for the second group can be derived, and it is same as that of the first group.

Since \mathbf{F}_2 is semi-unitary, there exists a unitary $T \times T$ matrix $\tilde{\mathbf{F}}_2$ such that $\tilde{\mathbf{F}}_2^H \mathbf{F}_2 = \begin{bmatrix} \mathbf{I}_N \\ \mathbf{0} \end{bmatrix}$. Consider the new STBC \mathcal{C}' obtained by multiplying all the weight matrices of the original STBC on the left by $\mathbf{C} = \begin{bmatrix} \mathbf{I}_T & \mathbf{0} \\ \mathbf{0} & i\tilde{\mathbf{F}}_2^H \end{bmatrix}$. Then, the lower submatrix of all the weight matrices of the second group are of the form $\begin{bmatrix} \pm \mathbf{I}_N \\ \mathbf{0} \end{bmatrix}$. Since the lower submatrix of every matrix in the first group is Hurwitz-Radon orthogonal to $\begin{bmatrix} \pm \mathbf{I}_N \\ \mathbf{0} \end{bmatrix}$, the weight matrices in the first group of \mathcal{C}' have the following structure: $\begin{bmatrix} \mathbf{V}_1 \\ \mathbf{B} \\ \mathbf{E} \end{bmatrix}$, where $\mathbf{V}_1 = \pm \mathbf{F}_1$, \mathbf{B} is an $N \times N$ Hermitian matrix and $\mathbf{E} \in \mathbb{C}^{\frac{T}{2}-N \times N}$. Let $\mathbf{B}_1, \dots, \mathbf{B}_{N^2}$ be any basis for the space of $N \times N$ Hermitian matrices over \mathbb{R} , $L = TN - 2N^2$ and $\mathbf{E}_1, \dots, \mathbf{E}_L$ be

$$\begin{bmatrix} 1 & 0 & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix}, \dots, \begin{bmatrix} 0 & 0 & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix},$$

$$\begin{bmatrix} i & 0 & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix}, \begin{bmatrix} 0 & i & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix}, \dots, \begin{bmatrix} 0 & 0 & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & i \end{bmatrix},$$

which is a standard basis for the space of $(\frac{T}{2} - N) \times N$ complex matrices over \mathbb{R} . Clearly the space spanned by the weight matrices of the first group of \mathcal{C}' is a subspace of the space spanned by the following $\frac{K}{2}$ linearly independent matrices:

$$\begin{bmatrix} \mathbf{F}_1 \\ \mathbf{0} \\ \mathbf{0} \end{bmatrix}, \begin{bmatrix} \mathbf{0} \\ \mathbf{B}_n \\ \mathbf{0} \end{bmatrix}, \text{ for } n = 1, \dots, N^2, \begin{bmatrix} \mathbf{0} \\ \mathbf{0} \\ \mathbf{E}_l \end{bmatrix}, \text{ for } l = 1, \dots, L. \quad (11)$$

From dimension count, it is clear that the matrices in (11) form a basis for the space spanned by the weight matrices of the first group of \mathcal{C}' . For

any non-zero channel realization $\mathbf{H} \in \mathbb{C}^{N \times M}$, the subspaces $\mathcal{V}_1 = \left\langle \begin{bmatrix} \mathbf{F}_1 \mathbf{H} \\ \mathbf{0} \\ \mathbf{0} \end{bmatrix} \right\rangle$, $\mathcal{V}_2 = \left\langle \begin{bmatrix} \mathbf{0} \\ \mathbf{B}_n \mathbf{H} \\ \mathbf{0} \end{bmatrix}, n = 1, \dots, N^2 \right\rangle$ and $\mathcal{V}_3 = \left\langle \begin{bmatrix} \mathbf{0} \\ \mathbf{0} \\ \mathbf{E}_l \mathbf{H} \end{bmatrix}, l = 1, \dots, L \right\rangle$ are such that their pairwise intersections contain only the all zero matrix. Thus, the rank of the equivalent channel matrix of the first group of \mathbf{C}' is

$$\text{rank}(\mathbf{G}'_1) = \dim(\mathcal{V}_1) + \dim(\mathcal{V}_2) + \dim(\mathcal{V}_3).$$

With probability 1, $\dim(\mathcal{V}_1) = 1$ and from Theorem 1, $\dim(\mathcal{V}_2) = f(N, M)$. It is straightforward to show that $\dim(\mathcal{V}_3) = (T - 2N) \cdot \min\{N, M\}$ with probability 1. From Proposition 1, we know that every STBC is non-singular for $M \geq N$. We thus consider only the case $M < N$. Then from Proposition 3, the rank of the equivalent channel matrix of the first ML decoding group of the STBC given in [12] is

$$\text{rank}(\mathbf{G}_1) = \text{rank}(\mathbf{G}'_1) = (T - 2N) \cdot M + f(N, M) + 1.$$

Compare this with the number of symbols in the first group $\frac{K}{2} = (T - 2N) \cdot N + N^2 + 1$. Thus, for any $M < N$, $\text{rank}(\mathbf{G}_1) < \frac{K}{2}$ with probability 1.

Using a similar argument it can be shown that the rank of the equivalent channel matrix of the second group also equals $(T - 2N) \cdot M + f(N, M) + 1$ with probability 1. Since, the two groups can be ML decoded independently of each other, the complexity of sphere decoding the STBC proposed in [12] is $\mathcal{O}(q^{(N-M) \cdot (T-N-M)})$ for any $M < N$ and the STBC is singular for all $\lceil R \rceil \leq M < N$.

Example 3: Consider the STBC from [12] for $N = 4$ and $T = 2N = 8$. The rate of this code is $R = \frac{17}{8}$ and the number of symbols per decoding group is $\frac{K}{2} = 17$. From the above discussion it is clear that this STBC is singular for $M = 3$. The rank of the equivalent channel matrix of each ML decoding group equals 16 with probability 1 and hence the sphere decoding complexity is $\mathcal{O}(q)$.

It is interesting to compare this code with the code from [10] which we have discussed in Section III-A and Example 1. Both codes have the same parameters N , R and both have a sphere decoding complexity that is linear in the constellation size q . However, the code in [10] is fast-group-decodable and 5 levels can be removed from the sphere decoding search tree of the second decoding group. Hence, after conditioning on the value taken by one of the real symbols (to account for the reduced rank of the equivalent channel matrix), the code in [10] uses a 10-dimensional sphere decoder to decode the second group of 16 symbols. For decoding each ML decoding group, the code from [12], uses a 16 dimensional search tree after conditioning on the value of one of the real symbols. Thus, the sphere decoding complexity of the code from [10] is less than that of [12].

D. Multigroup ML decodable codes from Natarajan et. al [14]

In [14], delay optimal g -group ML decodable codes were constructed for all $g > 1$, $N = ng2^{\lfloor \frac{g-1}{2} \rfloor}$, $n \geq 1$, with rate

$R = \frac{N}{g2^{g-1}} + \frac{g^2 - g}{2N}$. In this subsection we show that the sphere decoding complexity of the codes with even g is of the order of $q^{\left(\left(n-2^{\lfloor \frac{g-1}{2} \rfloor} M\right)^+\right)^2}$ and that the codes are non-singular only for $M \geq \frac{N}{g2^{g-2}}$. Also in [14], non-delay optimal codes with $T = gN$, $N = n2^{\lfloor \frac{g-1}{2} \rfloor}$, $n \geq 1$ were constructed. We show that the sphere decoding complexity of these codes for even values of g is of the order of $q^{\left(\left(n-2^{\lfloor \frac{g-1}{2} \rfloor} M\right)^+\right)^2}$. Simulation results show that the STBCs in [14] for odd values of g are also singular for certain number of receive antennas.

Delay-optimal codes: The number of symbols per group is $\frac{K}{g} = n^2 + g - 1$ and let $m = 2^{\lfloor \frac{g-1}{2} \rfloor}$. We will now derive the rank of the equivalent channel matrix \mathbf{G}_1 of the STBC corresponding to the first group. The weight matrices of the first group have a block diagonal structure $\text{diag}(\mathbf{D}_1, \mathbf{D}_2, \dots, \mathbf{D}_g)$, where each $\mathbf{D}_j \in \mathbb{C}^{nm \times nm}$. The first block \mathbf{D}_1 is one of the n^2 matrices of the form $\mathbf{V} \otimes \mathbf{U}_1$, where $\mathbf{V} \in \mathbb{C}^{n \times n}$ is Hermitian, and the remaining $g - 1$ matrices \mathbf{D}_j , $j = 2, \dots, g$ are of the form $\pm \mathbf{I}_n \otimes \mathbf{U}_j$ for some set of g unitary $m \times m$ matrices $\mathbf{U}_1, \dots, \mathbf{U}_g$. Let us multiply all the weight matrices of the first group on the right by $\mathbf{C} = \text{diag}(\mathbf{I}_n \otimes \mathbf{U}_1^H, \dots, \mathbf{I}_n \otimes \mathbf{U}_g^H)$. Clearly, the new set of weight matrices $\mathbf{A}'_1, \dots, \mathbf{A}'_{\frac{K}{g}}$ also have a block diagonal structure $\text{diag}(\mathbf{D}_1, \mathbf{D}_2, \dots, \mathbf{D}_g)$ where \mathbf{D}_1 is one of the n^2 matrices of the form $\mathbf{V} \otimes \mathbf{I}_n$, where \mathbf{V} is $n \times n$ Hermitian and the remaining $g - 1$ blocks are of the form $\pm \mathbf{I}_n \otimes \mathbf{I}_m$. It is straightforward to show that there exists a permutation matrix \mathbf{P} such that $\mathbf{P} \cdot (\mathbf{V} \otimes \mathbf{I}_m) \cdot \mathbf{P}^T = \mathbf{I}_m \otimes \mathbf{V}$ for any $\mathbf{V} \in \mathbb{C}^{n \times n}$. Consider the matrices $\mathbf{A}''_j = \mathbf{C}' \mathbf{A}'_j \mathbf{C}'^T$, $j = 1, \dots, \frac{K}{g}$, where $\mathbf{C}' = \text{diag}(\mathbf{P}, \mathbf{I}_{nm}, \dots, \mathbf{I}_{nm})$. Let $\mathbf{B}_1, \dots, \mathbf{B}_{n^2}$ be any basis for the space of $n \times n$ Hermitian matrices. From dimension count and the structure of the \mathbf{A}''_j matrices, $\langle \mathbf{A}''_1, \dots, \mathbf{A}''_{\frac{K}{g}} \rangle$ equals the span of the matrices $\hat{\mathbf{A}}_1, \dots, \hat{\mathbf{A}}_{\frac{K}{g}}$ which given by $\text{diag}(\mathbf{I}_m \otimes \mathbf{B}_l, \mathbf{0}, \dots, \mathbf{0})$, $l = 1, \dots, n^2$, $\text{diag}(\mathbf{0}, \mathbf{I}_{nm}, \mathbf{0}, \dots, \mathbf{0})$, \dots , $\text{diag}(\mathbf{0}, \dots, \mathbf{0}, \mathbf{I}_{nm})$. Since \mathbf{C}'^T is unitary, the statistics of \mathbf{H} and $\mathbf{C}'^T \mathbf{H}$ are same. Along with Propositions 2 and 3, it is thus clear that $\text{rank}(\mathbf{G}_1)$ has the same statistics as the rank of the equivalent channel matrix $\hat{\mathbf{G}}_1$ of the STBC whose weight matrices are $\hat{\mathbf{A}}_1, \dots, \hat{\mathbf{A}}_{\frac{K}{g}}$.

Let the channel realization be $\mathbf{H} = [\mathbf{H}_1^T \dots \mathbf{H}_g^T]^T$, where $\mathbf{H}_k \in \mathbb{C}^{nm \times M}$, $k = 1, \dots, g$. We are interested in the dimension of $\langle \hat{\mathbf{A}}_1 \mathbf{H}, \dots, \hat{\mathbf{A}}_{\frac{K}{g}} \mathbf{H} \rangle$ which is the span of

$$\begin{bmatrix} (\mathbf{I}_m \otimes \mathbf{B}_l) \mathbf{H}_1 \\ \mathbf{0} \\ \vdots \\ \mathbf{0} \end{bmatrix}, \text{ for } l = 1, \dots, n^2, \begin{bmatrix} \mathbf{0} \\ \mathbf{H}_2 \\ \vdots \\ \mathbf{0} \end{bmatrix}, \dots, \begin{bmatrix} \mathbf{0} \\ \mathbf{0} \\ \vdots \\ \mathbf{H}_g \end{bmatrix}. \quad (12)$$

Thus, with probability 1, $\text{rank}(\hat{\mathbf{G}}_1)$ equals the sum of $g-1$ and the dimension of the span of the first n^2 matrices in (12). Let us rewrite \mathbf{H}_1 as $[\mathbf{H}_{1,1}^T \dots \mathbf{H}_{1,m}^T]^T$, where $\mathbf{H}_{1,j} \in \mathbb{C}^{n \times M}$ for $j = 1, \dots, m$. Thus, the dimension of the span of first n^2

matrices in (12) is same as that of

$$\begin{bmatrix} \mathbf{B}_1 \mathbf{H}_{1,1} \\ \mathbf{B}_1 \mathbf{H}_{1,2} \\ \vdots \\ \mathbf{B}_1 \mathbf{H}_{1,m} \end{bmatrix}, \begin{bmatrix} \mathbf{B}_2 \mathbf{H}_{1,1} \\ \mathbf{B}_2 \mathbf{H}_{1,2} \\ \vdots \\ \mathbf{B}_2 \mathbf{H}_{1,m} \end{bmatrix}, \dots, \begin{bmatrix} \mathbf{B}_{n^2} \mathbf{H}_{1,1} \\ \mathbf{B}_{n^2} \mathbf{H}_{1,2} \\ \vdots \\ \mathbf{B}_{n^2} \mathbf{H}_{1,m} \end{bmatrix}.$$

This in turn, is equal to the dimension of the span of the following matrices

$$\begin{bmatrix} \mathbf{B}_1 \mathbf{H}_{1,1} & \mathbf{B}_1 \mathbf{H}_{1,2} & \cdots & \mathbf{B}_1 \mathbf{H}_{1,m} \end{bmatrix}, \\ \begin{bmatrix} \mathbf{B}_2 \mathbf{H}_{1,1} & \mathbf{B}_2 \mathbf{H}_{1,2} & \cdots & \mathbf{B}_2 \mathbf{H}_{1,m} \end{bmatrix}, \\ \vdots \\ \begin{bmatrix} \mathbf{B}_{n^2} \mathbf{H}_{1,1} & \mathbf{B}_{n^2} \mathbf{H}_{1,2} & \cdots & \mathbf{B}_{n^2} \mathbf{H}_{1,m} \end{bmatrix}.$$

From Theorem 1, this dimension equals $f(n, mM)$ with probability 1. Hence,

$$\text{rank}(\mathbf{G}_1) = \text{rank}(\hat{\mathbf{G}}_1) = f(n, mM) + g - 1$$

with probability 1. Compare this with the number of symbols per group $\frac{K}{g} = n^2 + g - 1$. Thus, the delay optimal STBCs of [14] for even values of g are singular whenever $\lceil R \rceil \leq M < \frac{n}{2^{\lfloor \frac{g-1}{2} \rfloor}}$. Similar results on the rank of the equivalent channel matrix can be proved for other ML decoding groups also. Thus, the sphere decoding complexity of these codes is of the order of $q^{\left(\left(n-2^{\lfloor \frac{g-1}{2} \rfloor} M\right)^+\right)^2}$. This STBC is singular only for $M \geq \frac{N}{g2^{g-2}} \approx 2R$. For $g = 2$, and equal values of N , the delay-optimal codes of [14] and the codes of [13] have equal rate and the same order of sphere decoding complexity.

Example 4: Consider the $g = 2$, $N = 6$ delay-optimal code of [14]. The underlying STBC has rate $R = \frac{5}{3}$ and there are $\frac{K}{2} = 10$ symbols per ML decoding group. From the ongoing discussion, for $M = 2$ receive antennas $\text{rank}(\mathbf{G}_k) = 9$ with probability 1 for $k = 1, 2$. Hence, this STBC is singular for $M = 2$ and the sphere decoding complexity is $\mathcal{O}(q)$. Let us denote the weight matrices of $\mathcal{C}_3^{\text{Herm}}$ given in Example 2 by $\mathbf{A}'_1, \dots, \mathbf{A}'_9$. Then, the 20 weight matrices of the $N = 6$, $g = 2$ code of [14] are given by

$$\mathbf{A}_\ell = \begin{bmatrix} i\mathbf{A}'_\ell & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_3 \end{bmatrix}, \ell = 1, \dots, 9, \quad \mathbf{A}_{10} = \begin{bmatrix} i\mathbf{A}'_1 & \mathbf{0} \\ \mathbf{0} & -\mathbf{I}_3 \end{bmatrix}, \\ \mathbf{A}_{\ell+10} = \begin{bmatrix} \mathbf{I}_3 & \mathbf{0} \\ \mathbf{0} & i\mathbf{A}'_\ell \end{bmatrix}, \ell = 1, \dots, 9, \quad \text{and} \quad \mathbf{A}_{20} = \begin{bmatrix} -\mathbf{I}_3 & \mathbf{0} \\ \mathbf{0} & i\mathbf{A}'_1 \end{bmatrix}.$$

Now consider the 24×20 \mathbf{G} matrix corresponding to the randomly generated channel realization

$$\mathbf{H} = \begin{bmatrix} -0.0583 + 1.2105i & 0.0708 + 0.6795i \\ -1.3669 - 0.1373i & -0.3850 + 0.0877i \\ -0.3104 - 1.5120i & 0.2146 + 1.0159i \\ -1.2690 - 0.5937i & -0.4245 - 1.3866i \\ 0.5942 + 0.9578i & 0.3465 - 0.1398i \\ -0.6279 - 0.7581i & 0.5228 - 0.8541i \end{bmatrix}.$$

The rank of \mathbf{G} is only 18 and the structure of the 24×20 upper triangular matrix \mathbf{R}' obtained from the QR decomposition is

given in (13) at the top of the next page. The matrix \mathbf{R}' is of the form $\begin{bmatrix} \mathbf{R}_1 & \mathbf{0}_{9 \times 10} \\ \mathbf{0}_{1 \times 10} & \mathbf{0}_{1 \times 10} \\ \mathbf{0}_{9 \times 10} & \mathbf{R}_2 \\ \mathbf{0}_{5 \times 10} & \mathbf{0}_{5 \times 10} \end{bmatrix}$, where $\mathbf{R}_1, \mathbf{R}_2 \in \mathbb{R}^{9 \times 10}$. The 10×10

all zero submatrix at the upper right corner of \mathbf{R}' is due to the 2-group ML decodability property of the code. The two sphere decoders corresponding to the two ML decoding groups use the matrices \mathbf{R}_1 and \mathbf{R}_2 respectively. Clearly the rank of \mathbf{R}_1 and \mathbf{R}_2 is 9, and hence the sphere decoding complexity is $\mathcal{O}(q)$.

Non delay-optimal codes: The non delay-optimal code for $N = n2^{\lfloor \frac{g-1}{2} \rfloor}$ has rate $R = \frac{N}{2^{g-1}} + \frac{g-1}{2N}$ and number of symbols per group $\frac{K}{g} = n^2 + g - 1$. The weight matrices of the first group are of the form $[\mathbf{D}_1^T, \mathbf{D}_2^T, \dots, \mathbf{D}_g^T]^T$, where each $\mathbf{D}_j \in \mathbb{C}^{nm \times nm}$. The first block \mathbf{D}_1 is one of the n^2 matrices of the form $\mathbf{V} \otimes \mathbf{U}_1$, where $\mathbf{V} \in \mathbb{C}^{n \times n}$ is Hermitian, and the remaining $g - 1$ matrices \mathbf{D}_j , $j = 2, \dots, g$ are of the form $\pm \mathbf{I}_n \otimes \mathbf{U}_j$ for some set of g unitary $m \times m$ matrices $\mathbf{U}_1, \dots, \mathbf{U}_g$.

Using an argument similar to the one used with delay-optimal codes, it can be shown that the sphere decoding complexity of the non delay optimal codes is of the order of $q^{\left(\left(n-2^{\lfloor \frac{g-1}{2} \rfloor} M\right)^+\right)^2}$ and that the codes are non-singular only for $M \geq \frac{N}{2^{g-2}} \approx 2R$. For $g = 2$ and equal values of N and T , the non-delay optimal codes of [14] and the codes of [12] have the same rate and sphere decoding complexity.

IV. DISCUSSION

In this paper we have introduced the notion of singularity of STBCs and showed that all known families of high rate multigroup ML decodable codes are singular for certain number of receive antennas. The following facts which were not known before have been shown.

- Though the $N = 4$, $T = 4$ code of [10] and the $N = 4$, $T = 8$ code of [12] have identical rate of $\frac{17}{8}$ cspcu, the sphere decoding complexity of the code from [10] is less than that of the code from [12].
- For $g = 2$, and equal values of N , the delay-optimal codes of [14] and the codes of [13] have equal rate and the same order of sphere decoding complexity.
- For equal values of N and T , the codes in [12] and the non-delay optimal codes of [14] have identical rate and sphere decoding complexities.

The results and ideas presented in this paper have brought to light the following important open problems.

- Is there an algebraic criterion that ensures that a code is non singular? For example, is every code with non vanishing determinant also non-singular for all $M \geq R$?
- Do there exist high rate multigroup ML decodable codes that are non-singular for arbitrary values of M ?
- Do there exist singular high rate multigroup ML decodable STBCs with lower sphere decoding complexity than that of the known codes?

$$\mathbf{R}' = \begin{bmatrix} a & a & a & a & a & a & a & a & a & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a & a & a & a & a & a & a & a & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & a & a & a & a & a & a & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a & a & a & a & a & a & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a & a & a & a & a & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & a & a & a & a & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & a & a & a & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a & a & a & a & a & a & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a & a & a & a & a & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a & a & a & a & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a & a & a & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a & a & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (13)$$

ACKNOWLEDGMENT

This work was supported partly by the DRDO-IISc program on Advanced Research in Mathematical Engineering through a research grant, and partly by the INAE Chair Professorship grant to B. S. Rajan

APPENDIX A PROOF OF THEOREM 1

From Proposition 1 it is clear that the theorem is true for $M \geq N$. Thus, we will only consider the case $M < N$. Before giving the proof of Theorem 1 we present two results which are used in the proof. Let $\mathbf{e}_1, \dots, \mathbf{e}_N$ be the N columns of the matrix \mathbf{I}_N .

Proposition 5: For any $i = 1, \dots, N$, with probability 1 (w.p.1), the vector \mathbf{e}_i does not belong to the column space of the channel matrix \mathbf{H} .

Proof: We first prove the result for $i = 1$. Let the channel realization $\mathbf{H} = \begin{bmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \end{bmatrix}$, where $\mathbf{H}_1 \in \mathbb{C}^{N-M \times M}$ and $\mathbf{H}_2 \in \mathbb{C}^{M \times M}$. Now, consider the matrix $\tilde{\mathbf{H}} = \begin{bmatrix} \mathbf{I}_{N-M} & \mathbf{H}_1 \\ \mathbf{0} & \mathbf{H}_2 \end{bmatrix} \in \mathbb{C}^{N \times N}$. We have, $\det(\tilde{\mathbf{H}}) = \det(\mathbf{I}_{N-M}) \cdot \det(\mathbf{H}_2) = \det(\mathbf{H}_2)$ which is non-zero w.p.1 [15]. Thus, w.p.1, the columns of $\tilde{\mathbf{H}}$ are linearly independent over \mathbb{C} , and since \mathbf{e}_1 is the first column of $\tilde{\mathbf{H}}$, this means that w.p.1, \mathbf{e}_1 does not belong to the column space of the matrix \mathbf{H} .

Now consider any $i \in \{1, \dots, N\}$. Let \mathbf{P} be an $N \times N$ permutation matrix such that $\mathbf{P}\mathbf{e}_i = \mathbf{e}_1$. Since \mathbf{P} is full-ranked,

\mathbf{e}_i belongs to the column space of \mathbf{H} if and only if \mathbf{e}_1 belongs to the column space of \mathbf{PH} . Since \mathbf{P} is unitary, the distribution of \mathbf{H} and \mathbf{PH} are one and the same, and hence the probability that \mathbf{e}_1 belongs to the column space of \mathbf{PH} is 0. Thus, with probability 1, \mathbf{e}_i does not belong to the column space of \mathbf{H} . ■

For a given channel realization \mathbf{H} , let $\mathcal{S} = \{\mathbf{z} \in \mathbb{C}^N | \mathbf{z}^H \mathbf{H} = \mathbf{0}\}$. Since \mathbf{H} is of rank M w.p.1, the dimension of \mathcal{S} over \mathbb{R} is equal to $2(N - M)$ w.p.1. Let $\mathbf{z} = [z_1 \ z_2 \ \dots \ z_N]^T$ and for $i = 1, \dots, N$, let $\varphi_i : \mathcal{S} \rightarrow \mathbb{R}$ be the vector space homomorphism that sends the vector \mathbf{z} to the real number $(z_i)_Q$. We are interested in the dimension of the subspace of \mathcal{S} which is composed of vectors whose i^{th} component is purely real, i.e., in the dimension of $\ker(\varphi_i)$.

Proposition 6: For $i = 1, \dots, N$, the dimension of image of \mathcal{S} under the map φ_i , $\dim(\ker(\varphi_i)) = 2(N - M) - 1$ w.p.1.

Proof: For any given \mathbf{H} , $\varphi_i(\mathcal{S}) \subset \mathbb{R}$ and hence $\dim(\varphi_i(\mathcal{S}))$ is either 0 or 1. Suppose, $\dim(\varphi_i(\mathcal{S})) = 0$, then, there is no vector \mathbf{z} in \mathcal{S} such that z_i is non-zero because if such a \mathbf{z} exists, the vector $iz_i^* \cdot \mathbf{z}$ belongs to \mathcal{S} and the imaginary part of its i^{th} component is $|z_i|^2 \neq 0$, and thus $\dim(\varphi_i(\mathcal{S})) = 1$, which is a contradiction. Since, for all the vectors in \mathcal{S} , the i^{th} component is 0, we have

$$\mathcal{S} = \{\mathbf{z} | \mathbf{z}^H \mathbf{H} = \mathbf{0}\} = \{\mathbf{z} | \mathbf{z}^H [\mathbf{H} \mathbf{e}_i] = \mathbf{0}\}.$$

Thus, the dimension of the column space of \mathbf{H} and $[\mathbf{H} \mathbf{e}_i]$ are the same. This means that \mathbf{e}_i belongs to the column space of \mathbf{H} . From Proposition 5, \mathbf{e}_i belongs to the column space of \mathbf{H} w.p.0 and hence $\dim(\varphi_i(\mathcal{S})) = 0$ w.p.0.

Thus, $\dim(\varphi_i(\mathcal{S})) = 1$ w.p.1. From rank-nullity theorem, $\dim(\ker(\varphi_i)) = \dim(\mathcal{S}) - \dim(\varphi_i(\mathcal{S})) = 2(N - M) - 1$ w.p.1. ■

Proof of Theorem 1: Let the weight matrices of the STBC $\mathcal{C}_N^{\text{Herm}}$ be $\mathbf{A}_1, \dots, \mathbf{A}_{N^2}$ and let the space of $N \times N$ Hermitian matrices over \mathbb{R} be given by $\mathcal{U} = \langle \mathbf{A}_1, \dots, \mathbf{A}_{N^2} \rangle$. For a given channel realization \mathbf{H} , let $\rho: \mathcal{U} \rightarrow \mathbb{C}^{N \times M}$ be the \mathbb{R} -vector space homomorphism that sends the matrix \mathbf{A} to $\mathbf{A}\mathbf{H}$. Clearly, $\text{rank}(\mathbf{G})$ is equal to the dimension of the subspace $\rho(\mathcal{U})$ over \mathbb{R} . Since $\rho(\mathcal{U})$ is isomorphic to $\mathcal{U}/\ker(\rho)$ as vector spaces, we have

$$\text{rank}(\mathbf{G}) = \dim(\mathcal{U}) - \dim(\ker(\rho)) = N^2 - \dim(\ker(\rho)).$$

Thus, it is enough to show that $\dim(\ker(\rho)) = (N - M)^2$ w.p.1. Let $\mathbf{A} \in \ker(\rho)$ and let $\mathbf{a}_1^H, \dots, \mathbf{a}_N^H$ denote the N rows of \mathbf{A} . Then, \mathbf{a}_1 satisfies $\mathbf{a}_1^H \mathbf{H} = \mathbf{0}$, and since the \mathbf{A} is Hermitian, the first component of \mathbf{a}_1 is purely real. From Proposition 6, $\mathbf{a}_1 \in \ker(\varphi_1)$ whose dimension is $2(N - M) - 1$ w.p.1. Given a choice of \mathbf{a}_1 , since \mathbf{A} is Hermitian, the first component of \mathbf{a}_2 equals the conjugate of the second component of \mathbf{a}_1 , and the second component of \mathbf{a}_2 is purely real. As a result of these restrictions and since $\mathbf{a}_2^H \mathbf{H} = \mathbf{0}$, i.e., $\mathbf{a}_2 \in \ker(\varphi_2)$, \mathbf{a}_2 belongs to a coset of the subspace of \mathcal{S} whose dimension is $(2(N - M) - 1) - 2 = 2(N - M) - 3$. Similarly, given a choice for $\mathbf{a}_1, \dots, \mathbf{a}_{k-1}$, where $k = 1, \dots, N$, the first $k - 1$ components of \mathbf{a}_k are fixed and the imaginary part of the k^{th} component is zero. Hence, \mathbf{a}_k belongs to a coset of a subspace of \mathcal{S} with dimension $(2(N - M) - 1) - 2k$. Thus, the dimension of $\ker(\rho)$ equals

$$2(N - M) - 1 + 2(N - M) - 3 + \dots + 1 = (N - M)^2,$$

with probability 1. This completes the proof. ■

REFERENCES

- [1] B. Hassibi and B. M. Hochwald, "High-Rate Codes that Are Linear in Space and Time," *IEEE Trans. Inf. Theory*, vol. 48, no. 7, pp. 1804-1824, Jul. 2002.
- [2] G. S. Rajan and B. S. Rajan, "Multi-group ML Decodable Collocated and Distributed Space Time Block Codes," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3221-3247, Jul. 2010.
- [3] H. Wang, D. Wang, and X.-G. Xia, "On Optimal Quasi-Orthogonal Space-Time Block Codes With Minimum Decoding Complexity," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1104-1130, Mar. 2009.
- [4] Z. A. Khan and B. S. Rajan, "Single Symbol Maximum Likelihood Decodable Linear STBCs," *IEEE Trans. Inf. Theory*, vol. 52, No. 5, pp. 2062-2091, May 2006.
- [5] L. P. Natarajan and B. S. Rajan, "Asymptotically-Optimal, Fast-Decodable, Full-Diversity STBCs," in Proc. of *IEEE ICC 2011*, Kyoto, Japan, June 06-09, 2011.
- [6] E. Viterbo and J. Boutros, "A Universal Lattice Code Decoder for Fading Channels," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1639-1642, Jul. 1999.
- [7] O. Damen, A. Chkeif, and J.-C. Belfiore, "Lattice Code Decoder for Space-Time Codes," *IEEE Comm. Letters*, vol. 4, no. 5, May 2000.
- [8] A. Y.-C. Peng, I.-M. Kim, and S. Yousefi, "Low-Complexity Sphere Decoding Algorithm for Quasi-Orthogonal SpaceTime Block Codes," *IEEE Trans. Comm.*, vol. 54, no. 3, March 2006.
- [9] M. O. Damen, H. El Gamal, and G. Caire, "On Maximum-Likelihood Detection and the Search for the Closest Lattice Point," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2389-2402, Oct. 2003.
- [10] T. P. Ren, Y. L. Guan, C. Yuen, and R. J. Shen, "Fast-Group-Decodable Space-Time Block Code," in Proc. of *IEEE ITW 2010*, Cairo, Egypt, Jan. 06-08, 2010.
- [11] C. Yuen, Y. L. Guan, and T. T. Tjhung, "On the search for high-rate quasi-orthogonal space-time block code," *Int. J. Wireless Inf. Network (IJWIN)*, vol. 13, pp. 329-340, Oct. 2006.
- [12] T. P. Ren, C. Yuen, Y. L. Guan, E. Gunawan, and E. Y. Zhang, "Unbalanced and Balanced 2-Group Decodable Spatial Multiplexing Code," in Proc. of *IEEE VTC (Fall)*, 2009.
- [13] K. P. Srinath and B. S. Rajan, "High-Rate, 2-Group ML-Decodable STBCs for 2^m Transmit Antennas," in Proc. of *IEEE ISIT 2009*, Seoul, South Korea, June 28- July 03, 2009, pp. 2008-2012.
- [14] L. P. Natarajan and B. S. Rajan, "Asymptotically-Good, Multigroup ML-Decodable STBCs," in Proc. of *IEEE Globecom 2010*, Miami, Florida, USA, Dec. 06-10, 2010.
- [15] D. Tse and P. Viswanath, "Fundamentals of Wireless Communication," Cambridge, U.K.: Cambridge University Press, 2005.
- [16] K. P. Srinath and B. S. Rajan, "Low ML-Decoding Complexity, Large Coding Gain, Full-Rate, Full-Diversity STBCs for 2x2 and 4x2 MIMO Systems," *IEEE J. Sel. Topics Signal Process.*, vol. 3, No. 6, pp. 916 - 927, Dec. 2009.